



UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
-----------------	-------------	----------------------	---------------------	------------------

09/406,087

09/24/1999

RYOTA AKIYAMA

1341.1030/JD

1217

21171

7590

05/19/2006

STAAS & HALSEY LLP

SUITE 700

1201 NEW YORK AVENUE, N.W.

WASHINGTON, DC 20005

EXAMINER

BROWN, CHRISTOPHER J

ART UNIT

PAPER NUMBER

2134

DATE MAILED: 05/19/2006

Please find below and/or attached an Office communication concerning this application or proceeding.

Office Action Summary	Application No. 09/406,087	Applicant(s) AKIYAMA ET AL.	
	Examiner Christopher J. Brown	Art Unit 2134	

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE 3 MONTH(S) OR THIRTY (30) DAYS, WHICHEVER IS LONGER, FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

- 1) ☒ Responsive to communication(s) filed on 28 February 2006.
- 2a) ☒ This action is **FINAL**. 2b) ☐ This action is non-final.
- 3) ☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

- 4) ☒ Claim(s) 27-43 and 45 is/are pending in the application.
- 4a) Of the above claim(s) _____ is/are withdrawn from consideration.
- 5) ☐ Claim(s) _____ is/are allowed.
- 6) ☒ Claim(s) 27-43, 45 is/are rejected.
- 7) ☐ Claim(s) _____ is/are objected to.
- 8) ☐ Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

- 9) ☐ The specification is objected to by the Examiner.
- 10) ☐ The drawing(s) filed on _____ is/are: a) ☐ accepted or b) ☐ objected to by the Examiner.
Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).
Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).
- 11) ☐ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

Priority under 35 U.S.C. § 119

- 12) ☐ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).
- a) ☐ All b) ☐ Some * c) ☐ None of:
1. ☐ Certified copies of the priority documents have been received.
2. ☐ Certified copies of the priority documents have been received in Application No. _____.
3. ☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).
- * See the attached detailed Office action for a list of the certified copies not received.

Attachment(s)

- | | |
|---|---|
| 1) <input type="checkbox"/> Notice of References Cited (PTO-892) | 4) <input type="checkbox"/> Interview Summary (PTO-413) |
| 2) <input type="checkbox"/> Notice of Draftsperson's Patent Drawing Review (PTO-948) | Paper No(s)/Mail Date. _____ |
| 3) <input type="checkbox"/> Information Disclosure Statement(s) (PTO-1449 or PTO/SB/08) | 5) <input type="checkbox"/> Notice of Informal Patent Application (PTO-152) |
| Paper No(s)/Mail Date _____ | 6) <input type="checkbox"/> Other: _____ |

DETAILED ACTION

Response to Arguments

1. Applicant's arguments filed 2/28/06 have been fully considered but they are not persuasive.

The applicant argues that Kitaori does not teach that the function is a one-way function. Kitaori teaches that the function is a MD5, or SHA hash, both of which are well known one way functions, (Col 8 lines 9-14).

The applicant argues that Olarig US 6,009,524 does not teach applying two digital signatures, or one way functions, to data. The applicant argues that the vendors key is "merely used for verification purposes". This is irrelevant with regards to the instant specification. Olarig teaches applying a first digital signature to data with a first key, and subsequently applying a second digital signature to the data using a second key. The method relied on for the digital signing is found in Kitaori US 5,915,024, which states that a signature or hash is attached to each of a divided data (Col 8 lines 5-22, Fig 4).

Included below is the previous office action, and rejection of new claim 45.

Claim Rejections - 35 USC § 102

2. The following is a quotation of the appropriate paragraphs of 35 U.S.C. 102 that form the basis for the rejections under this section made in this Office action:

A person shall be entitled to a patent unless –

Art Unit: 2134

(e) the invention was described in a patent granted on an application for patent by another filed in the United States before the invention thereof by the applicant for patent, or on an international application by another who has fulfilled the requirements of paragraphs (1), (2), and (4) of section 371(c) of this title before the invention thereof by the applicant for patent.

The changes made to 35 U.S.C. 102(e) by the American Inventors Protection Act of 1999 (AIPA) and the Intellectual Property and High Technology Technical Amendments Act of 2002 do not apply when the reference is a U.S. patent resulting directly or indirectly from an international application filed before November 29, 2000. Therefore, the prior art date of the reference is determined under 35 U.S.C. 102(e) prior to the amendment by the AIPA (pre-AIPA 35 U.S.C. 102(e)).

Claim 45 is rejected under 35 U.S.C. 102(e) as being anticipated by Kitaori US 5,915,024.

As per claim 45 Kitaori teaches a first authenticator creating unit (transmitting terminal) for dividing the information into a plurality of data (divided document data) (Col 7 lines 61-66). Kitaori discloses that the authenticators are created by applying one-way functions (hashes, signatures) to each of the divided data, (Col 8 lines 5-22).

Kitaori teaches linking the authenticators to the divided data (Col 8 lines 32-38, Fig 4).

Claim Rejections - 35 USC § 103

3. The following is a quotation of 35 U.S.C. 103(a) which forms the basis for all obviousness rejections set forth in this Office action:

(a) A patent may not be obtained though the invention is not identically disclosed or described as set forth in section 102 of this title, if the differences between the subject matter sought to be patented and the prior art are such that the subject matter as a whole would have been obvious at the time the invention was made to a person

Art Unit: 2134

having ordinary skill in the art to which said subject matter pertains. Patentability shall not be negated by the manner in which the invention was made.

Claims 27, 32, and 37-43 are rejected under 35 U.S.C. 103(a) as being unpatentable over Kitaori US 5,915,024 in view of Olarig US 6,009,524

As per claims 27, 32, and 37-43 Kitaori teaches a first authenticator creating unit (transmitting terminal) for dividing the information into a plurality of data (divided document data) (Col 7 lines 61-66). Kitaori discloses that each has a prespecified length (delimiter character), (Col 7 lines 24-27). Kitaori discloses that the authenticators are created by applying a one-way function (hash, signature) to each of the divided data, (Col 8 lines 5-22).

Kitaori teaches linking the authenticator to the divided data (Col 8 lines 32-38). Kitaori discloses a certifying unit that recalculates the authenticator and checking to see that the recalculated authenticator data matches the send authenticator data, (Col 10 lines 1-40). Kitaori does not disclose using a different key and algorithm to create a one-way hash on each of the divided data.

Olarig teaches using two different signatures with different keys on data, (Col 4 lines 4-15). Olarig teaches verification of the signatures at the recipient, (Col 4 lines 15-20). It would be obvious to one skilled in the art to modify the signing system and message of Kitarori with the multiple algorithm and keys of Olarig to enhance the security of the message.

Claims 28, and 33 are rejected under 35 U.S.C. 103(a) as being unpatentable over Kitaori US 5,915,024 in view of Olarig US 6,009,524 in view of Herbert US 6,023,509

As per claims 28, and 33, Kitaori teaches a first authenticator creating unit (transmitting terminal) for dividing the information into a plurality of data (divided document data) (Col 7 lines 61-66). Kitaori discloses that each has a prespecified length (delimiter character), (Col 7 lines 24-27). Kitaori discloses that the authenticators are created by applying a one-way function (hash, signature) to each of the divided data, (Col 8 lines 5-22).

Kitaori teaches linking the authenticator to the divided data (Col 8 lines 32-38). Kitaori discloses a certifying unit that recalculates the authenticator and checking to see that the recalculated authenticator data matches the send authenticator data, (Col 10 lines 1-40). Kitaori does not disclose using a different key and algorithm to create a one-way hash on each of the divided data.

Olarig teaches using two different signatures with different keys on data, (Col 4 lines 4-15). Olarig teaches verification of the signatures at the recipient, (Col 4 lines 15-20). It would be obvious to one skilled in the art to modify the signing system and message of Kitarori with the multiple algorithm and keys of Olarig to enhance the security of the message.

Neither Kitarori or Olarig teach creating a signature by hashing both a first result and a second data division.

Art Unit: 2134

Herbert teaches a method that involves creation of a digital signature through a first hash in combination with a second data division, to create an authenticator, (Col 3 lines 15-24).

It would have been obvious to one of ordinary skill in the art to use the previous system of Kitarori-Olarig with the digital signature of Herbert, because it provides advantageous purpose binding (Col 3 lines 33-36).

Claims 29, 31, 34, and 36 are rejected under 35 U.S.C. 103(a) as being unpatentable over Kitaori US 5,915,024 in view of Olarig US 6,009,524 in view of Dolan US 5,604,801

As per claims 29, 31, 34 and 36, the previous Kitaori-Olarig combination does not disclose truncation. Dolan discloses generating a digital signature made up of an encrypted hash of the message, (Col 6 lines 1-12). The digital signature is made of the original message, and the authenticators, thus the authenticators are truncated to the information.

It would be obvious to modify the Kitaori-Olarig combination with Dolan's digital signature so the receiver will be able to authenticate the sender, thus making the transmission more secure.

As per claims 3, and 8, Shear teaches using a first and second key different from each other to create authenticators, (Col 16 lines 30-36).

Art Unit: 2134

Claims 30 and 35 are rejected under 35 U.S.C. 103(a) as being unpatentable over

Kitaori US 5,915,024 in view of Olarig US 6,009,524 in view of Bellare US 5,757,913

As per claims 30 and 35, the previous Kitaori-Olarig combination does not disclose parallel processing.

Bellare discloses parallel processing, (Col 1 lines 60-65).

It would have been obvious to one of ordinary skill in the art to modify the Kitaori-Olarig combination with Bellare's parallel processing to improve speed and efficiency.

Conclusion

4. Applicant's amendment necessitated the new ground(s) of rejection presented in this Office action. Accordingly, **THIS ACTION IS MADE FINAL**. See MPEP § 706.07(a). Applicant is reminded of the extension of time policy as set forth in 37 CFR 1.136(a).

A shortened statutory period for reply to this final action is set to expire **THREE MONTHS** from the mailing date of this action. In the event a first reply is filed within **TWO MONTHS** of the mailing date of this final action and the advisory action is not mailed until after the end of the **THREE-MONTH** shortened statutory period, then the shortened statutory period will expire on the date the advisory action is mailed, and any extension fee pursuant to 37 CFR 1.136(a) will be calculated from the mailing date of the advisory action. In no event, however, will the statutory period for reply expire later than **SIX MONTHS** from the date of this final action.

Art Unit: 2134

Any inquiry concerning this communication or earlier communications from the examiner should be directed to Christopher J. Brown whose telephone number is (571)272-3833. The examiner can normally be reached on 8:30-6:00.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Jaques Louis Jaques can be reached on (571)272-6962. The fax phone number for the organization where this application or proceeding is assigned is 571-273-8300.

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see <http://pair-direct.uspto.gov>. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free).

Christopher J. Brown

5/14/06

